RECEIVED
CENTRAL FAX CENTER
APR 1 3 2007

Amendments to the Claims:

1-30. (Cancelled)

31. (Currently amended) A system for protecting a distributed network from unauthorized access, the system comprising:

an intrusion detection system, including:

an intrusion detection module, and

a communications management module coupled to the intrusion detection module; and

intrusion analysis system coupled to the intrusion detection system, and including:

an intrusion analysis module, and

an intrusion reaction coordination module coupled to the intrusion analysis module,

wherein the intrusion detection module detects a possible unauthorized access attempt into or within a distributed network being protected,

the communications management module is coupled to the intrusion analysis module and forwards to the intrusion analysis module information regarding the detected possible unauthorized access attempt,

the intrusion analysis module determines based on the information regarding the detected possible unauthorized access attempt whether or not the detected possible unauthorized access attempt is authorized,

if the intrusion analysis module determines that the detected possible unauthorized access attempt is authorized, the intrusion analysis module forwards, via the communications management module, information to the intrusion detection module that the possible unauthorized access attempt is authorized, and

if the intrusion analysis module determines that the detected possible unauthorized access attempt is not authorized, the intrusion analysis module determines, via the intrusion reaction coordination module, appropriate actions, including forwarding information regarding the detected unauthorized access attempt to a monitoring center external to the distributed network being protected, and processing information from the monitoring center regarding the detected unauthorized access attempt,

wherein the intrusion analysis system in cooperation with the intrusion detection system enable communications between the monitoring center and an entity attempting the unauthorized access attempt without the entity being made aware that the entity attempting the unauthorized access attempt is communicating with the monitoring center, ~~and~~

wherein the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the unauthorized access attempt and forwards the substituted information to the entity attempting the unauthorized access attempt, whereby it appears to the entity attempting the unauthorized access attempt that communications are continuing with the target of the unauthorized access attempt, and

wherein the intrusion analysis system in cooperation with the intrusion detection system engages the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt.

32. (Cancelled)

33. (Currently amended) The system of claim 31 ~~32~~, wherein the intrusion analysis system communicates with monitoring center via a secure tunnel.

34. (Currently amended) The system of claim 31 ~~32~~, wherein the communications from the monitoring center to the entity attempting the unauthorized access attempt are modified, via the intrusion analysis system and the intrusion detection system, to appear as if the communications originate from the distributed network being protected.

35. (Currently amended) The system of claim 31 ~~32~~, wherein the intrusion analysis system logs information regarding communications with the entity attempting the unauthorized access attempt.

36. (Cancelled)

37. (Cancelled)

38. (Previously presented) The system of claim 31, wherein the intrusion detection module detects whether or not the possible unauthorized access attempt into or within the distributed network being protected is internal or external to the network being protected.

39. (Previously presented) The system of claim 31, wherein if the intrusion detection module detects that the possible unauthorized access attempt is internal to the network being protected, the intrusion detection module forwards via the communications management module information regarding the possible internal unauthorized access attempt to the intrusion analysis module, and the intrusion analysis module evaluates the received information and if the intrusion analysis module determines that the possible internal unauthorized access attempt is not authorized, the intrusion analysis module determines whether or not a retaliatory action should be taken, including handling the unauthorized access attempt internally or providing information to the monitoring center regarding the unauthorized access attempt.

40. (Previously presented) The system of claim 31, wherein the monitoring center comprises a law enforcement entity.

41. (Previously presented) The system of claim 31, further comprising a database,

wherein the intrusion analysis module employs the database, including information regarding previous unauthorized access attempts, to determine whether or not the detected possible unauthorized access attempt is authorized.

42. (Previously presented) The system of claim 41, wherein the database includes profiles of information related to one or more entities associated with the previous unauthorized access attempts, including origin information regarding the previous unauthorized access attempts.

43. (Previously presented) The system of claim 41, wherein the intrusion analysis module is configured to query the database to determine whether or not the possible unauthorized access attempt is an error in communications, including a bit error.

44. (Previously presented) The system of claim 31, wherein the intrusion analysis module is configured to determine based on historical profiles, and previous unauthorized access attempts whether or not the detected possible unauthorized access attempt is authorized.

45. (Previously presented) The system of claim 31, wherein the intrusion reaction coordination module determines the appropriate actions based on a number of previous unauthorized access attempts, and a nature of the unauthorized access attempt, including destructiveness of packets received during the unauthorized access attempt.

46. (Previously presented) The system of claim 31, wherein the intrusion reaction coordination module, to determine the appropriate actions, analyzes the information received by the intrusion detection module, historical information regarding unauthorized access attempts, source and destination ports of unauthorized access attempts, IP address information of unauthorized access attempts, and information received from a central repository that catalogs information related to unauthorized access attempts from one or more other protected networks.

47. (Previously presented) The system of claim 46, wherein the analysis is based on at least one of a look-up table, a neural network analysis, and a predetermined event sequence.

48. (Previously presented) The system of claim 31, wherein if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module instructs the intrusion detection module to block communications from an entity attempting the unauthorized access attempt.

49. (Previously presented) The system of claim 31, wherein if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module instructs the intrusion detection module to block communications from an entity that matches one or more characteristics of the unauthorized access attempt.

50. (Previously presented) The system of claim 41, wherein the intrusion reaction coordination module logs information regarding an entity attempting the unauthorized access attempt to the database for use in a future unauthorized access attempt by the entity.

51. (Previously presented) The system of claim 31, wherein the intrusion analysis module system is configured to store information regarding an address to which the unauthorized access attempt was directed for use by the intrusion reaction coordination module to determine the appropriate actions.

52. (Previously presented) The system of claim 41, wherein upon receipt of a communication from the monitoring center, the intrusion detection system in cooperation with the intrusion analysis system analyze the communication, determine address information of a source of the communication from the monitoring center, and removes the address information from the communication from the monitoring center leaving the remaining information for further analysis.

53. (Previously presented) The system of claim 52, wherein the address information of the source of the communication from the monitoring center is stored in the database, and the intrusion analysis module is configured to use the address information to communicate information to the monitoring center, including information regarding a response to a password request by an entity attempting the unauthorized access attempt.

54. (Currently amended) The system of claim 31 ~~32~~, wherein the intrusion detection system in cooperation with the intrusion analysis system conceal an identity of the monitoring center, communicate information with the monitoring center, and screen

underlying content in the communicated information, including removing sensitive information from the communicated information.

55. (Previously presented) The system of claim 54, wherein the intrusion detection system in cooperation with the intrusion analysis system employ a policy file to regulate the screening and removing of the sensitive information, including removing all content or core information, removing content having certain words, and removing content originating from a predetermined location.

56. (Previously presented) The system of claim 31, wherein the intrusion detection system and the intrusion analysis system cooperate with the monitoring center to aid in detecting a source of the unauthorized access attempt.

57. (Previously presented) The system of claim 56, wherein the intrusion detection system in cooperation with the intrusion analysis system receive from the monitoring center information regarding unauthorized accesses or access attempts into distributed networks.

58. (Previously presented) The system of claim 57, wherein the intrusion detection system in cooperation with the intrusion analysis system analyze the information regarding unauthorized accesses or access attempts into the distributed networks received from the monitoring center to determine if the received information matches a profile or has characteristics corresponding to one or more known unauthorized access attempts.

59. (Previously presented) The system of claim 58, wherein, upon detection of an unauthorized access attempt, the intrusion detection system in cooperation with the intrusion analysis system forward information regarding the unauthorized access attempt to the monitoring center for inclusion in a central database that maintains the information regarding the unauthorized accesses or access attempts into the distributed networks.

60. (Previously presented) The system of claim 31, wherein the system is implemented with one or more hardware and or software components.

61. (Currently amended) A method for protecting a distributed network from unauthorized access for use in a system including an intrusion detection system having an intrusion detection module, and a communications management module coupled to the intrusion detection module, and intrusion analysis system coupled to the intrusion detection system, and including an intrusion analysis module, and an intrusion reaction coordination module coupled to the intrusion analysis module, the method comprising:

detecting, by the intrusion detection module, a possible unauthorized access attempt into or within a distributed network being protected;

forwarding, by the communications management module, information regarding the detected possible unauthorized access attempt to the intrusion analysis module;

determining, by the intrusion analysis module, based on the information regarding the detected possible unauthorized access attempt whether or not the detected possible unauthorized access attempt is authorized;

if the intrusion analysis module determines that the detected possible unauthorized access attempt is authorized, forwarding, by the intrusion analysis module, via the communications management module, information to the intrusion detection module that the possible unauthorized access attempt is authorized, and

if the intrusion analysis module determines that the detected possible unauthorized access attempt is not authorized, determining, by the intrusion analysis module, via the intrusion reaction coordination module, appropriate actions, including forwarding information regarding the detected unauthorized access attempt to a monitoring center external to the distributed network being protected, and processing information from the monitoring center regarding the detected unauthorized access attempt,

wherein the intrusion analysis system in cooperation with the intrusion detection system enable communications between the monitoring center and an entity attempting the unauthorized access attempt without the entity being made aware that the entity attempting the unauthorized access attempt is communicating with the monitoring center, ~~and~~

wherein the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin

information of a target of the unauthorized access attempt and forwards the substituted information to the entity attempting the unauthorized access attempt, whereby it appears to the entity attempting the unauthorized access attempt that communications are continuing with the target of the unauthorized access attempt, and

wherein the intrusion analysis system in cooperation with the intrusion detection system engages the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt.

62. (Cancelled)

63. (Currently amended) The method of claim 61 ~~62~~, wherein the intrusion analysis system communicates with monitoring center via a secure tunnel.

64. (Currently amended) The method of claim 61 ~~62~~, wherein the communications from the monitoring center to the entity attempting the unauthorized access attempt are modified, via the intrusion analysis system and the intrusion detection system, to appear as if the communications originate from the distributed network being protected.

65. (Currently amended) The method of claim 61 ~~62~~, wherein the intrusion analysis system logs information regarding communications with the entity attempting the unauthorized access attempt.

66. (Cancelled)

67. (Cancelled)

68. (Previously presented) The method of claim 61, wherein the intrusion detection module detects whether or not the possible unauthorized access attempt into or within the distributed network being protected is internal or external to the network being protected.

69. (Previously presented) The method of claim 61, wherein if the intrusion detection module detects that the possible unauthorized access attempt is internal to the network being protected, the intrusion detection module forwards via the communications management module information regarding the possible internal unauthorized access attempt to the intrusion analysis module, and the intrusion analysis module evaluates the received information and if the intrusion analysis module determines that the possible internal unauthorized access attempt is not authorized, the intrusion analysis module determines whether or not a retaliatory action should be taken, including handling the unauthorized access attempt internally or providing information to the monitoring center regarding the unauthorized access attempt.

70. (Previously presented) The method of claim 61, wherein the monitoring center comprises a law enforcement entity.

71. (Previously presented) The method of claim 61, further comprising a database, wherein the intrusion analysis module employs the database, including information regarding previous unauthorized access attempts, to determine whether or not the detected possible unauthorized access attempt is authorized.

72. (Previously presented) The method of claim 71, wherein the database includes profiles of information related to one or more entities associated with the previous unauthorized access attempts, including origin information regarding the previous unauthorized access attempts.

73. (Previously presented) The method of claim 71, wherein the intrusion analysis module is configured to query the database to determine whether or not the possible unauthorized access attempt is an error in communications, including a bit error.

74. (Previously presented) The method of claim 61, wherein the intrusion analysis module is configured to determine based on historical profiles, and previous unauthorized

access attempts whether or not the detected possible unauthorized access attempt is authorized.

75. (Previously presented) The method of claim 61, wherein the intrusion reaction coordination module determines the appropriate actions based on a number of previous unauthorized access attempts, and a nature of the unauthorized access attempt, including destructiveness of packets received during the unauthorized access attempt.

76. (Previously presented) The method of claim 61, wherein the intrusion reaction coordination module, to determine the appropriate actions, analyzes the information received by the intrusion detection module, historical information regarding unauthorized access attempts, source and destination ports of unauthorized access attempts, IP address information of unauthorized access attempts, and information received from a central repository that catalogs information related to unauthorized access attempts from one or more other protected networks.

77. (Previously presented) The method of claim 76, wherein the analysis is based on at least one of a look-up table, a neural network analysis, and a predetermined event sequence.

78. (Previously presented) The method of claim 61, wherein if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module instructs the intrusion detection module to block communications from an entity attempting the unauthorized access attempt.

79. (Previously presented) The method of claim 61, wherein if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module instructs the intrusion detection module to block communications from an entity that matches one or more characteristics of the unauthorized access attempt.

80. (Previously presented) The method of claim 71, wherein the intrusion reaction coordination module logs information regarding an entity attempting the unauthorized access attempt to the database for use in a future unauthorized access attempt by the entity.

81. (Previously presented) The method of claim 61, wherein the intrusion analysis module system is configured to store information regarding an address to which the unauthorized access attempt was directed for use by the intrusion reaction coordination module to determine the appropriate actions.

82. (Previously presented) The method of claim 71, wherein upon receipt of a communication from the monitoring center, the intrusion detection system in cooperation with the intrusion analysis system analyze the communication, determine address information of a source of the communication from the monitoring center, and removes the address information from the communication from the monitoring center leaving the remaining information for further analysis.

83. (Previously presented) The method of claim 82, wherein the address information of the source of the communication from the monitoring center is stored in the database, and the intrusion analysis module is configured to use the address information to communicate information to the monitoring center, including information regarding a response to a password request by an entity attempting the unauthorized access attempt.

84. (Currently amended) The method of claim 61 ~~-62~~, wherein the intrusion detection system in cooperation with the intrusion analysis system conceal an identity of the monitoring center, communicate information with the monitoring center, and screen underlying content in the communicated information, including removing sensitive information from the communicated information.

85. (Previously presented) The method of claim 84, wherein the intrusion detection system in cooperation with the intrusion analysis system employ a policy file to regulate the screening and removing of the sensitive information, including removing all content or core

information, removing content having certain words, and removing content originating from a predetermined location.

86. (Previously presented) The method of claim 61, wherein the intrusion detection system and the intrusion analysis system cooperate with the monitoring center to aid in detecting a source of the unauthorized access attempt.

87. (Previously presented) The method of claim 86, wherein the intrusion detection system in cooperation with the intrusion analysis system receive from the monitoring center information regarding unauthorized accesses or access attempts into distributed networks.

88. (Previously presented) The method of claim 87, wherein the intrusion detection system in cooperation with the intrusion analysis system analyze the information regarding unauthorized accesses or access attempts into the distributed networks received from the monitoring center to determine if the received information matches a profile or has characteristics corresponding to one or more known unauthorized access attempts.

89. (Previously presented) The method of claim 88, wherein, upon detection of an unauthorized access attempt, the intrusion detection system in cooperation with the intrusion analysis system forward information regarding the unauthorized access attempt to the monitoring center for inclusion in a central database that maintains the information regarding the unauthorized accesses or access attempts into the distributed networks.

90. (Previously presented) The method of claim 61, wherein said method is implemented with one or more hardware and/or software devices configured to perform the steps of the method.

91. (Previously presented) The method of claim 61, wherein said method is implemented with one or more computer readable instructions embedded on a computer readable medium and configured to cause one or more computer processors to perform the steps of the method.